



Department of Homeland Security Daily Open Source Infrastructure Report for 21 August 2006

Current
Nationwide
Threat Level is

ELEVATED
SIGNIFICANT RISK OF
TERRORIST ATTACKS

[For info click here](http://www.dhs.gov/)

<http://www.dhs.gov/>

Daily Highlights

- The Associated Press reports utility officials said the theft of copper from a substation was responsible for a blackout that left several thousand households in Oklahoma City without power. (See item [1](#))
- HCA Inc. said ten computers containing Medicare and Medicaid billing information and thousands of files on employees and physicians were stolen from one of the company's regional offices. (See item [11](#))
- The Christian Science Monitor reports terrorism experts say that the West's war on terror is attracting more and more young Muslims to militant circles, meaning that al Qaeda may no longer be the primary enemy, but that disparate groups of young radicals are emerging as equally potent threats. (See item [44](#))

DHS Daily Open Source Infrastructure Report *Fast Jump*

Production Industries: [Energy](#); [Chemical Industry and Hazardous Materials](#); [Defense Industrial Base](#)

Service Industries: [Banking and Finance](#); [Transportation and Border Security](#); [Postal and Shipping](#)

Sustenance and Health: [Agriculture](#); [Food](#); [Water](#); [Public Health](#)

Federal and State: [Government](#); [Emergency Services](#)

IT and Cyber: [Information Technology and Telecommunications](#); [Internet Alert Dashboard](#)

Other: [Commercial Facilities/Real Estate, Monument & Icons](#); [General](#); [DHS Daily Report Contact Information](#)

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED

Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES-ISAC) – <http://www.esisac.com>]

1. *August 19, Associated Press* — **Copper theft leads to second power outage.** Utility officials blamed a blackout that left several thousand households in Oklahoma City, OK, without power on the theft of copper from a substation. The Friday, August 18, outage marked the second time

in two weeks that thieves broke into Oklahoma Gas and Electric Co. (OG&E) substations to steal copper, which is selling for near-record high prices. The latest outage apparently was caused by a stolen copper wire used to ground the substation equipment, OG&E spokesperson Brian Alford said. The theft is believed to have occurred late Thursday night or early Friday morning even though the power outage began about 3:30 Friday afternoon. The outage follows just eight days after someone broke into an OG&E power substation in Moore to steal copper from a transformer. That attempt shut off electricity for about 5,500 customers. Oklahoma Corporation Commissioner Denise Bode said, "This is critical infrastructure...When you're shutting down a substation or knocking out a transmission line, you have an impact on a segment of the economy and the infrastructure that's being supplied." The commission is working with the state Department of Homeland Security, the Oklahoma Sheriff's Association, and other groups to curtail thefts.

Source: <http://www.kotv.com/news/?109641>

2. *August 19, Statesman Journal (OR)* — **Reward offered in power-outage case.** The Bonneville Power Administration (BPA) is offering a reward of as much as \$25,000 to find the people responsible for a four-hour power outage to the Consumers Power's Lebanon substation on Tuesday, August 15. Vandals shot out insulators on a transmission line about 11 miles east of Lebanon, OR, BPA officials said.
Source: <http://www.statesmanjournal.com/apps/pbcs.dll/article?AID=/20060819/NEWS/608190315>
3. *August 18, Democrat Herald (OR)* — **Vandalism ruled out as cause of outage.** Vandalism has been ruled out as the cause of the Wednesday, August 16, wide-spread power outage in the Albany and Corvallis areas of Oregon. There was no gunshot, as one rumor suggested, and no evidence that a car had struck a pole, said Pacific Power spokesperson Bekki Witt. The outage was caused by a broken insulator at the Hazelwood substation on Queen Avenue in West Albany. The outage left nearly 43,000 Pacific Power customers without power for more than an hour.
Source: <http://www.democratherald.com/articles/2006/08/18/news/local /friloc03.txt>
4. *August 17, Caspar Star Tribune (WY)* — **Wyoming coal-to-liquid plant advances.** From concept and siting, an effort to build one of the nation's first coal-to-liquids plants in Wyoming will soon move to the permitting and design stage. Medicine Bow Fuel & Power LLC recently awarded a contract to Canadian firm SNC-Lavalin to perform feasibility, engineering, and design services for a \$1 billion facility located in northern Carbon County. Plans are for initial production at 11,000 barrels per day of liquid hydrocarbons, 85 percent of which would be ultra-low-sulfur diesel sold as a consumer transportation fuel in the Rocky Mountain Region. Robert Kelly of Medicine Bow Fuel & Power said, "We have enough (coal) reserves there (at the Medicine Bow location) to expand production to about 33,000 barrels per day of petroleum product...One thing the U.S. needs right now is domestic hydrocarbons, and we're going to make it out of coal and reduce our dependence on foreign oil."
Source: http://www.helenair.com/articles/2006/08/17/national/a060817 06_01.txt
5. *August 17, Associated Press* — **Texas breaks record with electricity demand.** Texans set a record for electricity use Thursday, August 17, for the second time in more than four weeks. The Electric Reliability Council of Texas (ERCOT) oversees the power grid for most of Texas.

ERCOT says 63,056 megawatts were used from 4 p.m. to 5 p.m. CDT. That broke the record of 62,396 set on July 17th. ERCOT spokesperson Dottie Roark says there were no problems with service, and ERCOT expected no problems over the weekend because load typically drops off on Friday and throughout the weekend. Temperatures on Thursday reached as high as 107 degrees.

Source: http://www.team4news.com/Global/story.asp?S=5296790&nav=menu_90_3

6. *August 16, Associated Press* — **New Alaska oil leases being offered.** The Department of the Interior (DOI) is set to open a vast area of environmentally sensitive wetlands in Alaska to new oil drilling, even as opponents point to corroding pipelines to the east at Prudhoe Bay as a reason to keep the area off-limits. Government geologists believe at least two billion barrels of oil and huge amounts of natural gas lie beneath the coastal lagoons, river deltas, and sedge grass meadows. Within days, DOI will open tracts in the lake area for leasing; winning bids will be announced in late September. The lake and its surrounding wetlands are within the 22 million acre federal National Petroleum Reserve–Alaska (NPPRA). Unlike the Arctic National Wildlife Refuge farther to the east, the NPPRA is acknowledged by all sides to be an area for energy development.

Source: http://www.washingtonpost.com/wp-dyn/content/article/2006/08/16/AR2006081600965_pf.html

[[Return to top](#)]

Chemical Industry and Hazardous Materials Sector

Nothing to report.

[[Return to top](#)]

Defense Industrial Base Sector

Nothing to report.

[[Return to top](#)]

Banking and Finance Sector

7. *August 17, Register (UK)* — **Florida man indicted over Katrina phishing scam.** A Florida man has been charged with setting up a phishing Website that sought to cash-in on the victims of Hurricane Katrina. Jovany Desir allegedly tried to trick sympathetic people into handing over banking details through a bogus American Red Cross Website. Desir is further charged with selling phishing tackle that allowed other ID crooks to establish bogus Websites more easily for approximately \$150 each. Desir was indicted over these alleged offenses, as well as establishing phony banking and online payment sites between July and October 2005, by a federal grand jury in Western Pennsylvania, the Associated Press reports. Targets of his alleged scams included PNC Bank in Pittsburgh, eBay, PayPal, and two Canadian financial organizations as well as the Red Cross, the Pittsburgh Tribune–Review adds. Prosecutors allege one of the bogus Canadian banking Websites, purportedly representing Banque Nationale, was visited 8,500 times by users apparently searching for the legitimate site. The five-count

indictment omits an estimate of how much Desir might have gained through his various alleged scams.

Source: http://www.channelregister.co.uk/2006/08/18/hurricane_k_phis_hing_scam/

8. *August 17, Seattle Post-Intelligencer* — **Shop owner arrested in debit card scam.** Redmond, WA, police have arrested the owner of a local smoke shop after dozens of customers who used their debit cards at his store discovered that their bank accounts had been siphoned. Some victims suffered \$900 in losses. Others took hits as high as \$3,000, police said. So far, investigators have identified at least 26 victims who were customers of US Bank and Washington Mutual, police records show. The 35-year-old suspect in this case is believed to be part of a large crime ring operating along the West Coast and in Nevada. The Tuesday arrest marks another case of suspected identity theft involving "skimming" and "cloning" of magnetic stripe information. Police believe the owner of Smoker's Choice, in the Overlake area, stole financial information from skimming customers' cards, but also somehow captured their PINs. With that information, withdrawals were made from casinos in Las Vegas and California, said Officer Stacey Holland. Police estimate monetary losses in excess of \$100,000.

Source: http://seattlepi.nwsources.com/local/281571_cardfraud17.html

9. *August 17, Post-Standard (NY)* — **BAE Systems hacked; Rome, New York, office says Social Security numbers may be compromised.** A defense contractor that works on classified government information at the former Griffiss Air Base in Rome has notified employees that someone hacked into its computer system. BAE Systems National Security Solutions Inc. on August 2 notified 4,500 current and former employees, retirees, and consultants that a Trojan virus had been found on a company computer server. The company employs 100 in Rome. July 18, the company discovered someone obtained unauthorized access to a company computer server at its main office in San Diego, CA. The server contained the names, addresses Social Security numbers, birth dates, telephone numbers, maiden names, and personal vehicle information. No personal financial information was on the computer. BAE hasn't identified the party who accessed the computer or if they were trying to gain access to personal or business information. It also can't determine if the virus stole personal information, but so far BAE has not received any reports of misused information.

Source: <http://www.syracuse.com/business/poststandard/index.ssf?/base/business-4/1155805278120570.xml&coll=1>

10. *August 17, Tampa Bay Business Journal (FL)* — **Florida bank reports bogus checks.** Community National Bank of Sarasota County, FL, told federal regulators that counterfeit checks issued in the bank's name are being presented for payment in connection with an Internet purchase scam. The Office of the Comptroller of the Currency (OCC) said the counterfeit items can be identified because the instruments are cream in color, the bank's logo appears faded, the word "No." does not appear in front of the check number, the reverse side of the check contains endorsement instructions, lines for signatures and the words "Federal Reserve Board of Governor Reg. CC." The checks use correct routing and account numbers and are being presented for payment locally and nationally, the OCC said in a release. Law enforcement says that the checks are originating out of Ghana, Africa.

Source: http://www.bizjournals.com/tampabay/stories/2006/08/14/daily_45.html

11.

August 17, Associated Press — **Ten stolen HCA computers contained patient, doctor, worker records.** HCA Inc. said ten computers containing Medicare and Medicaid billing information and records of employees and physicians were stolen from one of the company's regional offices. HCA officials won't say where or when the theft occurred because they believe that might help the thieves, who authorities believe were after computer hardware, not personal identity information. The FBI is investigating. The computers held thousands of files on Medicare and Medicaid patients treated at HCA hospitals in Colorado, Kansas, Louisiana, Mississippi, Oklahoma, Oregon, Texas, or Washington state between 1996 and 2006. The machines contained some patient names and Social Security numbers but no addresses or dates of birth. HCA spokesperson Jeff Prescott said on Thursday, August 17, the company had also discovered that the names and Social Security numbers of about 7,000 employees and physicians in four states — Colorado, Kansas, Louisiana and Texas — were on the computers. HCA is notifying those affected by letter.

Source: <http://www.siliconvalley.com/mld/siliconvalley/news/editorial/15298403.htm>

12. *August 15, Federal Financial Institutions Examination Council* — **FFIEC releases Frequently Asked Questions on guidance regarding Internet banking authentication.** The Federal Financial Institutions Examination Council (FFIEC) on Thursday, August 17, released a frequently asked questions document (FAQs) to aid in the implementation of the interagency guidance on Authentication in an Internet Banking Environment issued October 12, 2005. The authentication guidance, which applies to both retail and commercial customers, addresses the need for risk-based assessment, customer awareness, and security measures to reliably authenticate customers remotely accessing their financial institutions' Internet-based financial services. The FAQs are designed to assist financial institutions and their technology service providers in conforming to the guidance by providing information on the scope of the guidance, the timeframe for compliance, risk assessments, and other issues.

FFIEC FAQs: http://www.ffiec.gov/pdf/authentication_faq.pdf

Source: <http://www.ffiec.gov/press/pr081506.htm>

[\[Return to top\]](#)

Transportation and Border Security Sector

13. *August 20, Associated Press* — **Bomb squad sweeps plane, man questioned.** Bomb-sniffing dogs swept a Delta Air Lines flight from Atlanta upon landing in San Antonio on Saturday, August 19, after authorities said a passenger tampered with a smoke detector and moved ceiling panels in a lavatory. The passenger, a San Antonio man who was not identified, was being questioned by federal authorities at San Antonio International Airport, FBI spokesperson Erik Vasys said. The passenger on Delta Flight 6492 was overheard being "disruptive" in the lavatory by flight attendants and had spent an extended amount of time there, said Transportation Security Administration spokesperson Jennifer Peppin. The man had apparently tampered with the smoke detector, Vasys said. Authorities said ceiling tiles had also been moved. A bomb-sniffing dog that inspected the lavatory upon landing "showed some interest," airport spokesperson David Hebert said. A bomb squad then swept the plane but found no suspicious materials, he said.

Source: http://www.usatoday.com/travel/news/2006-08-20-passenger-detained_x.htm

14. *August 18, Associated Press* — **British plane makes emergency landing after bomb suspected on board.** A British passenger plane en route to an Egyptian resort made an emergency landing Friday in Brindisi, southern Italy, after the pilot reported that a bomb was suspected to be on board, the Italian air traffic agency said. All passengers disembarked and were safe, state police at the airport said. Excel said the captain made the decision to land in Italy after a passenger found a note written on the back of an airsickness bag that read: "There's a bomb on this aircraft." Excel Airways official Jane Sebuliba called the landing "a precautionary diversion." Italy's Air Force said it sent an F-16 to escort the plane to the airport. The airline said that all security checks were followed at London's Gatwick airport prior to departure. The plane, carrying 269 passengers and nine crewmembers, was diverted to Brindisi three hours later. Salvatore De Paolis, a border police officer at the Brindisi airport, said authorities searching the plane had recovered a handwritten note in English that said there was a bomb on the plane. The ENAV agency said the plane, a Boeing 767 with Excel Airways, was bound for the large Hurghada resort in Egypt.
Source: http://www.usatoday.com/news/world/2006-08-18-italy-plane_x.htm
15. *August 18, Reuters* — **Airport security rules eased for some business travel.** Tighter airport security in the wake of a foiled bomb plot in Britain last week sent big-spending business travelers rushing to private jets in hopes of avoiding long delays and luggage restrictions. But experts say the passenger migration from commercial airlines to private services will be short-lived as long as new government-imposed restrictions don't permanently impede the ability of travelers to work in airports and on planes. Business travelers, who often pay more for last-minute bookings and premium in-flight services, are a key revenue source for major airlines like AMR Corp's American Airlines and UAL Corp's United Airlines, which have invested heavily in business cabin improvements. Private jet services have seen a surge in business from travelers who could afford them. One expert said that if the inconveniences become the norm, airlines catering to business travelers could face persistent competition from private jet services. NBTA surveys show a growing use of private jets and charters since the 2001 terror attacks on the United States. A 2002 survey of corporate travel managers showed that 26 percent of U.S. companies used private jets. By 2004, 33 percent of the companies said they used them.
Source: http://www.usatoday.com/travel/flights/2006-08-18-private-jets_x.htm
16. *August 18, Associated Press* — **Midwest flight delayed over bottle of water.** A Midwest Airlines plane about to leave Milwaukee bound for Kansas City, MO, but returned from the runway to the gate because of a bottle of water. A flight attendant noticed a man with a bottle of water on Wednesday afternoon. He said he needed the water to take medicine, but the crew turned the plane around because of security rules. The crew later learned the Transportation Security Administration had allowed the man to bring the water on the plane, Midwest spokesperson Carol Skonicka said.
Source: http://www.usatoday.com/travel/flights/2006-08-17-water-delay_x.htm
17. *August 18, Associated Press* — **Man in marital spat disrupts flight from Fort Smith.** A Fort Smith, AR, man was jailed after calling in a bomb threat to the Fort Smith airport in an effort to keep his wife and two children from boarding a plane and leaving Arkansas. The FBI filed a complaint against Michael Terrell Jackson, 30, after Jackson allegedly called in a threat to the Fort Smith Regional Airport. FBI spokesperson Steve Frazier said it appeared Jackson's wife's

plane was never in danger. "It was a marital dispute. He was not a terrorist," Frazier said. "He was arrested ... on a federal complaint for making a threat to blow up a plane in an attempt to prevent his wife and two children from leaving Arkansas." Fort Smith police said Jackson called an airport security official Tuesday and said there were bombs on two planes going to Texas, then challenged the official to "find them if you can." An American Eagle flight scheduled for 1:34 p.m. departure to Dallas–Fort Worth was the only plane going to Texas, and it was cleared for flight after being checked by a bomb squad and an FBI agent.

Source: http://www.usatoday.com/travel/news/2006-08-18-fake-bomb-threat_x.htm

18. *August 18, USA TODAY* — **Boeing to end in-flight Internet service.** Aerospace giant Boeing said Thursday, August 17, that it can't find a buyer for its unit that sells high-speed broadband service to airlines and will shut it down by the end of the year. The decision to close the unit, Connexion by Boeing, ends the only in-flight Internet service for commercial airline travelers. The announcement disappoints, but doesn't completely surprise, customers such as German carrier Lufthansa. Chicago-based Boeing said in June that it would sell or shut down Connexion, which has been losing money since it was created in 2000. "I think Connexion may have been a product slightly of ahead of its times," says Henry Harteveldt, analyst at Forrester Research. "Boeing bears a lot of responsibility for its failure to make the equipment viable for single-aisle planes. It was too heavy and too expensive." Boeing will maintain the satellite-based service until the end of the year for its 10 airline customers: Lufthansa, Singapore, SAS, El Al, All Nippon, Japan Airlines, Asiana, China Air, Etihad Airways, and Korean Air. No U.S. airline is a customer.

Source: http://www.usatoday.com/travel/flights/2006-08-17-boeing-internet_x.htm

19. *August 18, Associated Press* — **Alaska Airlines jet diverted to Seattle after cabin fails to pressurize.** An Alaska Airlines jetliner was diverted to Seattle after the plane's cabin failed to pressurize normally Friday, August 18, during a flight from Canada, an airline spokesperson said. The Boeing 737 landed safely at Seattle–Tacoma International Airport, where medics treated 10 passengers and three crewmembers complaining of ear and sinus pain, airline spokesperson Amanda Tobin Bielawski said. Four people were taken to a hospital. An altitude warning alarm sounded when Flight 690 reached 33,000 feet, indicating a problem with the air pressure inside the cabin, Bielawski said. She said the plane's oxygen masks did not deploy. Earlier this year, Alaska ordered a fleet-wide inspection of its planes' air pressure systems after a series of similar cabin pressure problems. The company said no system-wide problems were found.

Source: http://www.usatoday.com/travel/news/2006-08-18-alaska-air-diverts_x.htm

[[Return to top](#)]

Postal and Shipping Sector

20. *August 18, DM News* — **USPS generates net deficiency for June.** The U.S. Postal Service (USPS) generated a net deficit of \$11.9 million before escrow allocation during June, according to financial and operating statements. The Civil Service Retirement System (CSRS) Funding Act requires the USPS to place \$3 billion in an escrow account by September 30 to cover the difference between the CSRS retirement costs before and after the law's implementation. The USPS said it is allocating \$250 million monthly for purposes of reconciling its financial

position. After the escrow allocation, the postal service's net deficiency for June becomes \$261.9 million. USPS revenue for June was \$5.94 billion, or 0.4 percent under plan and 5.6 percent more than June 2005. Expenses for the month were \$5.96 billion, or 0.7 percent under plan and 4.4 percent more than June 2005. Year-to-date revenue through June is 3.9 percent higher than the same period last year and is \$386 million above plan. Year-to-date expenses are 4.2 percent higher than the year-ago period and \$222 million over plan.

Source: <http://www.dmnews.com/cms/dm-news/direct-mail/37943.html>

[[Return to top](#)]

Agriculture Sector

21. *August 18, Stop Soybean Rust News* — **New soybean rust finds in Louisiana.** Asian soybean rust was confirmed Friday, August 18, on soybeans in Iberia and St. Mary parishes in Louisiana. On August 15, soybean rust was confirmed in two parishes, Avoyelles and Tensas, on soybeans. On Friday, August 11, 2006, soybean rust was found in a sentinel plot of soybeans in Natchitoches Parish. Currently rust has been found infecting this year's soybeans in 12 different counties in Alabama, Florida, Georgia, Louisiana and Mississippi. Including reports on kudzu, there is a total of 32 counties with rust this year, including five in Alabama, 13 in Florida, six in Georgia, six in Louisiana, one in Mississippi, and one in Texas.

Source: <http://www.stopsoybeanrust.com/viewStory.asp?StoryID=920>

22. *August 18, BBC News (UK)* — **Bluetongue virus hits Dutch farm.** The Dutch Government has banned all exports of live sheep, cattle and goats after a farm tested positive for the harmful bluetongue virus. Officials have also introduced movement restrictions. It is the first time the insect-borne virus, which is normally found in Mediterranean regions, has been discovered in northern Europe. All species of ruminants, which include goats and deer as well as cattle, can be infected. Sheep are the most susceptible, with up to 70 percent of an infected flock dying from the virus. "We have one farm with sheep that have bluetongue, and there are 10 farms with suspected cases of the disease," the Dutch Agriculture Ministry spokesperson said. Transportation of animals has been banned in a 12-mile radius around the affected farm, and farmers are being told to keep their animals indoors and to spray insecticides on their land. There are also restrictions on the movement of animals that can be infected beyond a wider 105-mile exclusion zone. Farmers in this area are also being told to spray insecticides.

Bluetongue information: <http://www.fao.org/AG/AGAINFO/subjects/en/health/diseases-cards/bluetongue.html>

Source: <http://news.bbc.co.uk/1/hi/sci/tech/5263456.stm>

23. *August 17, Mississippi State University* — **Agriculture exports rebound from shipping trouble.** Hurricane Katrina changed the way Mississippi crops leave the state, and some producers are still dealing with the change. Mississippi's port at Gulfport and the ports at New Orleans and Mobile served as the exit point for much of the state's crops. Katrina damaged each of these, wiping the Port of Gulfport clear of all its structures and temporarily closing the others. Nearly a year later, all are back in some level of operation, but Gulfport is still in the worst shape of the three. The Port of New Orleans handled about half of the state's grain exports before Katrina. Much of the nation's grain came down the Mississippi River and was shipped out from this port. Steve Martin, agricultural economist with the Mississippi State

University Extension Service, estimated that those exports have regained most of their pre-Katrina status. Martin said the river system is running smoothly now to handle this fall's harvests, assuming river levels do not drop too much lower.

Source: <http://msucares.com/news/print/agnews/an06/060817.html>

[[Return to top](#)]

Food Sector

24. *August 19, Agence France–Presse* — **Indian state files case against Coke alleging high pesticide levels.** India's southern state of Karnataka has filed a case against U.S. soft drink manufacturer Coca-Cola, accusing it of selling products with illegally high pesticide levels. The case was filed August 12 after state-supervised private laboratory tests showed excessive amounts of pesticide in Coca-Cola samples, Karnataka Health Minister Ashok said Saturday, August 19. The case was the first to be filed by a state government against Coke since a New Delhi-based environmental group said earlier this month that tests of products made by Coca-Cola and PepsiCo showed high pesticide levels. The allegations have turned into a publicity nightmare for the soft-drinks multinationals with six states, including Karnataka, imposing partial or full or bans on their products. Coca-Cola and PepsiCo, account for nearly 80 percent of India's two billion-dollar-a-year soft drinks market.
Source: http://news.yahoo.com/s/afp/20060820/wl_sthasia_afp/indiahea_lthcokecompany_060820000358
25. *August 19, Interfax (Russia)* — **Russia bans imports of poultry meat from Michigan.** Russia has banned poultry meat deliveries from Michigan. The decision was taken because bird flu virus of the H5 type was found in a swan in Michigan, the Federal Veterinary and Phytosanitary Control Service said. The ban will be active until the strain is established and the spot of the disease is localized, the minister said.
Source: http://www.interfax.ru/e/B/politics/28.html?id_issue=1157457_1
26. *August 19, Associated Press* — **First use of viruses as a food additive approved.** A mix of bacteria-killing viruses may be sprayed on cold cuts, wieners and sausages to combat common microbes that kill hundreds of people a year, federal health officials ruled Friday, August 18. The ruling, by the U.S. Food and Drug Administration, is the first approval of viruses as a food additive. The approved mix of six viruses is intended to be sprayed onto ready-to-eat meat and poultry products. The viruses, called bacteriophages, are meant to kill strains of the *Listeria monocytogenes* bacterium. The bacterium can cause a serious infection called listeriosis, primarily in pregnant women, newborns and adults with weakened immune systems. In the U.S., an estimated 2,500 people become seriously ill with listeriosis each year. Of those, 500 die.
Source: http://www.nytimes.com/2006/08/19/us/19viruses.html?_r=1&oref=slogin
27. *August 18, Food Safety and Inspection Service* — **Beef products recalled.** Dinner Bell Meat Products, Inc. a Lynchburg, VA, firm, is voluntarily recalling approximately 909 pounds of beef that may be contaminated with *E. coli* O157:H7, the U.S. Department of Agriculture's Food Safety and Inspection Service (FSIS) announced Friday, August 18. The problem was

discovered through company testing. FSIS has received no reports of illnesses associated with consumption of this product. The products were distributed to retail establishments and a distributor in southern Virginia. E. coli O157:H7 is a potentially deadly bacterium that can cause bloody diarrhea and dehydration.

Source: http://www.fsis.usda.gov/News & Events/Recall_027_2006_Release/index.asp

[[Return to top](#)]

Water Sector

28. *August 20, Chicago Tribune* — **Illness shuts Six Flags water park.** The water park at Six Flags Great America remained closed Saturday, August 19, after the Illinois Department of Public Health's announcement Friday, August 18, that four people had become sick after visits to the park. There were two confirmed and two possible cases of cryptosporidium infection found in visitors to the park. Cryptosporidium, which can cause diarrhea, fever and vomiting, is a common cause of waterborne disease within humans in the U.S.

Source: <http://www.chicagotribune.com/news/local/chicago/chi-0608200282aug20.1.2917998.story?coll=chi-newslocalchicago-hed&track=1&cset=true>

29. *August 18, Los Angeles Times* — **Radioactive leak reaches nuclear plant's groundwater.** Radioactive, cancer-causing tritium has leaked into the groundwater beneath San Onofre nuclear power plant, prompting the closure of one drinking water well in Orange County, CA, authorities said. Officials have not found evidence that the leak from the San Onofre Nuclear Generating Station, California's largest, has contaminated the drinking water supply. As a precaution, San Clemente officials shut down and are testing a city well near the contaminated area. In recent years, tritium leaks have been found at more than a dozen nuclear plants across the nation, prompting the Nuclear Regulatory Commission to form a task force to study the cause of the contamination.

Source: <http://www.latimes.com/news/local/la-me-radioactive18aug18.0.3580491.story?page=1&coll=la-home-local>

30. *August 17, U.S. Geological Survey* — **Chemical quality of self-supplied domestic well water.** U.S. Geological Survey (USGS) scientists evaluated a range of inorganic and organic contaminants in domestic wells from every state and Puerto Rico. Inorganic compounds arsenic (11 percent) and nitrate (eight percent) exceeded the U.S. Environmental Protection Agency's drinking water standards in well water most often while uranium, mercury, and fluoride also exceeded standards at a smaller percentage. Organic compounds rarely exceeded drinking water standards; however, atrazine, metolochlor, simazine, MTBE and chloroform were all detected in more than five percent of the wells sampled. Since the water quality of domestic wells is not federally regulated or nationally monitored, this study provides a previously nonexistent perspective on the quality of the self-supplied drinking water resources used by 45 million Americans. This national reconnaissance study is based on a compilation of existing data from a very large number of wells sampled as part of multiple USGS programs.

Report: http://health.usgs.gov/dw_contaminants/domestic_wells/focus_and_others_2006.pdf

Source: <http://www.usgs.gov/newsroom/article.asp?ID=1540>

[[Return to top](#)]

Public Health Sector

31. *August 20, Agence France–Presse* — **Indonesia confirms bird flu death, probes possible cluster.** A 35-year-old woman was Indonesia's 46th bird flu death, health authorities said as they stepped up an urgent probe into whether she may belong to a feared cluster of cases. The woman came from Cikelet, a group of villages in West Java's Garut district where two other people — one of whom remains alive — have been confirmed as being infected with H5N1. At least 16 others are being tested. Three other people from Cikelet have also died recently while exhibiting possible bird flu symptoms but were not tested for the virus, heightening concern that limited human-to-human transmission may have occurred in the area. Such cluster cases raise the chance of the virus mutating to become easily transmissible between humans.
Source: http://news.yahoo.com/s/afp/20060820/wl_asia_afp/healthfluindonesia_060820110004
32. *August 19, Agence France–Presse* — **Indian state to probe vaccine efficacy after rise in polio cases.** India's northern state of Uttar Pradesh has asked the national government to check the efficacy of a World Health Organization supplied polio vaccine after recording a sharp rise in polio cases. Uttar Pradesh, India's most populous state, has reported 185 polio cases so far this year, up from 29 for all of 2005. Officials say 75 percent of the polio-infected children had been inoculated against the disease. India's campaign against polio was launched in 1993 and was aimed at eradicating the disease by 2000, but was extended after the target was missed. The country launched an immunization drive targeting 45 million children in July after the new cases were detected.
Global Polio Eradication Initiative: <http://www.polioeradication.org/>
Source: http://news.yahoo.com/s/afp/20060819/hl_afp/healthindiapolio_060819130559
33. *August 18, U.S. Food and Drug Administration* — **Manufacturer ordered to cease production of human cells, tissues and cellular and tissue-based products.** The U.S. Food and Drug Administration (FDA) Friday, August 18, ordered Donor Referral Services (DRS), a human tissue-recovery firm, of Raleigh, NC, and its owner, Philip Guyett, to immediately cease all manufacturing operations, and to retain human cells, tissues, and cellular and tissue-based products (HCT/Ps) after an inspection found serious deficiencies in its manufacturing practices, including those governing donor screening and record keeping. The order to cease manufacturing and retain HCT/Ps requires DRS and Philip Guyett to immediately suspend any and all manufacturing steps, including but not limited to the recovery and shipment of HCT/Ps. FDA's inspection identified serious violations of the regulations, including the failure to establish and maintain procedures for manufacturing steps performed by DRS. In addition to the above stated violations, FDA also found several instances where records provided by DRS to another HCT/P establishment were at variance with the official death certificates FDA had obtained from the state where the death occurred.
Source: <http://www.fda.gov/bbs/topics/NEWS/2006/NEW01433.html>
34. *August 17, Reuters* — **Drug side effects to be tracked.** Methods used to track disease outbreaks also may be used to help spot side effects from prescription drugs after they hit the market, U.S. health officials said on Thursday, August 17. The U.S. Food and Drug Administration (FDA) agreed to work with the Massachusetts Institute of Technology on adapting technology to detect side effects earlier than current FDA monitoring systems. The

project will involve automated scanning of databases for unusual patterns of health problems that could be drug-related, said Scott Gottlieb, FDA deputy commissioner for medical and scientific affairs. It will build on computerized systems public health officials use to spot infectious disease outbreaks, follow the spread of influenza or detect a bioterrorist attack, he said.

Source: http://today.reuters.com/news/articleinvesting.aspx?type=governmentFilingsNews&storyID=2006-08-17T211705Z_01_N17284021_RTRIDST_0_HEALTH-FDA.XML

[[Return to top](#)]

Government Sector

Nothing to report.

[[Return to top](#)]

Emergency Services Sector

35. *August 18, New York Times* — Report calls for tighter rules in nursing home evacuations.

Frail elderly residents who were evacuated from nursing homes in the Gulf States suffered more than the vast majority of those who were not moved during last year's hurricanes, according to a report to be issued Friday, August 18, by the inspector general for the Department of Health and Human Services. The report is based on site visits and interviews with administrators and staff members at 20 nursing homes in Alabama, Florida, Louisiana, Mississippi and Texas, all with emergency plans that meet the requirements of federal and state law. But it found that the plans had rampant deficiencies, especially in ensuring the safe and comfortable evacuation of residents with complex needs. The report is the first federal effort to examine in detail the effectiveness of federally mandated emergency preparedness plans in nursing homes.

Full-text report: <http://www.oig.hhs.gov/oei/reports/oei-06-06-00020.pdf>

Source: <http://www.nytimes.com/2006/08/18/us/18prepare.html?n=Top%2fReference%2fTimes%20Topics%2fOrganizations%2fH%2fHealth%20and%20Human%20Services%20Department>

36. *August 18, Casper Star-Tribune (WY)* — Qwest plans 911 upgrade in Wyoming following August 1 outage. Qwest Communications International Inc. has announced plans to upgrade its 911 delivery system in Wyoming, largely to prevent a repeat of the August 1 outage that left much of the state without service for hours. The upgrade will add a layer of redundancy to the fiber cable system but will not increase capacity, said Mike Ceballos, president for Qwest in Wyoming. Meanwhile, the state Public Service Commission is preparing to initiate a "formal investigatory process" into the outage. The August 1 outage interrupted 911 services to about 134,000 of the less than 200,000 phone lines Qwest serves in Wyoming. Full service was restored about seven hours later.

Source: <http://www.casperstartribune.com/articles/2006/08/18/news/wyoming/e1f2281204d48cd8872571ce000397d1.txt>

37. *August 18, Advocate (LA)* — **Baton Rouge mayor worried about evacuation plan.** Federal officials from the Department of Homeland Security are working on a plan with Amtrak to evacuate people from New Orleans to Baton Rouge in case of another emergency. Baton Rouge Mayor-President Kip Holden said he is worried the new plan will make a bad situation even worse if thousands of evacuees pour into Baton Rouge during a crisis. However, according to JoAnne Moreau, director of the East Baton Rouge Office of Emergency Preparedness, Baton Rouge would simply be a short stop for 5,000 evacuees. Holden said that while the new plan may look good on paper, he will have to see it work to believe it can.
Source: <http://www.2theadvocate.com/news/3595001.html>

[[Return to top](#)]

Information Technology and Telecommunications Sector

38. *August 18, Security Focus* — **Mozilla Firefox, SeaMonkey, Camino, and Thunderbird multiple remote vulnerabilities.** The Mozilla Foundation has released thirteen security advisories specifying security vulnerabilities in Mozilla Firefox, SeaMonkey, Camino, and Thunderbird. These vulnerabilities allow attackers to: execute arbitrary machine code in the context of the vulnerable application; crash affected applications; run JavaScript code with elevated privileges, potentially allowing the remote execution of machine code; gain access to potentially sensitive information. Other attacks may also be possible.
For a complete list of vulnerable products: <http://www.securityfocus.com/bid/18228/info>
Solution: New versions of Firefox, SeaMonkey, Camino, and Thunderbird are available to address these issues. Most Mozilla applications have self-updating features that may be used to download and install fixes. For more information:
<http://www.securityfocus.com/bid/18228/references>
Source: <http://www.securityfocus.com/bid/18228/discuss>
39. *August 18, IDG News Service* — **AOL security tools raise adware questions.** Just days after posting details of searches made by hundreds of thousands of subscribers, AOL is in hot water again with consumer advocates. This time the issue is with the company's Active Virus Shield anti-virus software, released last week. The software's licensing agreement authorizes AOL to gather and share data on how the software is being used and permits AOL and its affiliates to send e-mail to users. Although security experts say that the Active Virus Shield does not behave in a malicious fashion or serve up unwanted ads, some are concerned that the product's end user license agreement (EULA) would allow AOL to send spam or serve up adware at some point in the future. "If it actually does any of the things stated in the EULA, we would actually flag it as spyware," said Christina Olson, a project manager with Stopbadware.org.
Source: http://www.infoworld.com/article/06/08/18/HNaoladware_1.html
40. *August 18, eWeek* — **Zero-day attackers target Japanese word processor.** According to a warning from anti-virus vendor Symantec, attackers are exploiting a previously undocumented vulnerability in Ichitaro, a word processor produced by Justsystems, a Japanese software company. Symantec virus researcher John Canavan said in an advisory that attackers were using maliciously rigged documents to exploit a unicode stack overflow in the software to execute code on the underlying operating system. He said the attack included the use of a Trojan horse named Infostealer.Papi, which is used to spy on the target system and relay

information back to the attackers. The Ichitaro attacks closely resemble the recent wave of zero-day attacks against Microsoft Office programs and suggest that corporate espionage may be the main motive.

Symantec advisory: http://www.symantec.com/enterprise/security_response/weblog/2006/08/justsystems_ichitaro_0day_used.html

Source: <http://www.eweek.com/article2/0.1895.2005410.00.asp>

41. *August 17, Federal Computer Week* — CEO: Feds must adapt to new style of cyberwarfare.

Cyberwarfare is changing and network defense must change with it, said John Thompson, chief executive officer of Symantec, during a keynote speech at the Air Force Information Technology Conference. In the past, critical information was protected via a “suit of armor” approach in which layers of protection were added to keep information safe, Thompson said. But these layers restricted the data, hampering real-time use at the cost of mission performance. Cyberattacks have changed in recent years from amateur hackers seeking notoriety to organized criminal enterprises with financial or hostile goals, Thompson said. For example, large-scale virus or worm attacks have decreased from about 100 from 2002 to 2004 to six last year. Today’s cybercriminal is interested in “perpetrating silent, highly targeted attacks to steal sensitive personal, financial, and operational information,” he said. Therefore, going forward, effective cyberdefense will depend on a mixture of protecting information technology infrastructure, protecting the information itself and protecting the interactions among people using the information, Thompson said.

Source: <http://www.fcw.com/article95705-08-17-06-Web>

42. *August 16, BBC News (UK)* — Internet's ruling body renews U.S. links. The U.S. looks set to maintain its role as ultimate supervisor of the Internet's addressing systems until 2011. The U.S. Department of Commerce has signed a five-year deal with administrative body Internet Corporation for Assigned Names and Numbers that renews the body's role overseeing Internet domains.

Source: <http://news.bbc.co.uk/1/hi/technology/4799137.stm>

Internet Alert Dashboard

Current Port Attacks	
Top 10 Target Ports	1026 (win-rpc), 4672 (eMule), 57714 (---), 57715 (---), 445 (microsoft-ds), 62641 (---), 65530 (WindowsMite), 25 (smtp), 135 (epmap), 20753 (---)
Source: http://isc.incidents.org/top10.html ; Internet Storm Center	
To report cyber infrastructure incidents or to request information, please contact US-CERT at soc@us-cert.gov or visit their Website: www.us-cert.gov .	
Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it-isac.org/ .	

[[Return to top](#)]

Commercial Facilities/Real Estate, Monument & Icons Sector

43.

August 18, Associated Press — **Security increased after al Qaeda letter threatens to blow up Taj Mahal.** Soldiers were on 24-hour guard at the Taj Mahal after officials received a letter threatening to blow up the monument, officials said Friday, August 18. Authorities were investigating a handwritten letter received Thursday, August 17 — purportedly sent by an al Qaeda supporter — that said the terrorist group planned blasts at the 17th century monument, which drew nearly 2.5 million tourists last year. "Police are verifying the source of the letter," said Ashok Kumar, a senior government official in Uttar Pradesh state where the Taj Mahal is located. "The letter could be false but we cannot afford to be complacent." Tourists have been warned not to carry any liquids, including bottles of mineral water, to the fabled white marble structure located in the city of Agra, 130 miles from the Indian capital, New Delhi. Sandbag bunkers also have been set up outside the towering entrance gates, Kumar said.
Source: <http://www.foxnews.com/story/0.2933.209209.00.html>

[\[Return to top\]](#)

General Sector

44. *August 18, Christian Science Monitor* — **A new generation of jihad seekers.** While British investigators have revealed a trans-Atlantic plot to blow up as many as 12 U.S.-bound planes, their case against British and Pakistani suspects also reveals that the West's war on terror is attracting more and more young Muslims to militant circles, say terrorism experts. The U.S.-led Iraq war and American support for Israel's bombardment of Lebanon are serving to fertilize anger in segments of the Muslim world. And, they say, this means that al Qaeda may no longer be the primary enemy, but that disparate groups of young radicals who are imitating their tactics are emerging as equally potent threats. Marc Sageman, author of "Understanding Terror Networks" and a former CIA case officer, and other analysts say that while details on the alleged London plot are still scant, they would be surprised if it formally involved al Qaeda in the manner that 9/11 did. Instead, they say, satellite TV and the Internet have spread al Qaeda's message across the globe, allowing admirers and imitators of the group to set up operations on their own.

Source: <http://www.csmonitor.com/2006/0818/p01s04-woeu.html>

45. *August 18, Associated Press* — **Report: UK police find martyr tapes.** Several martyr videos were reportedly discovered on at least six laptops owned by some of the 23 suspects being questioned in the foiled terror plot to bomb as many as 10 jetliners bound for the United States. The British Broadcasting Corp., citing an unofficial police source, said Friday, August 18, that several videos of the type that suicide bombers sometimes leave had been found as part of the intense investigation into the alleged plot. Staff from every police force in the UK are working on the case, and dozens of specialist teams are continuing sweeps of homes, businesses and a stretch of dense woodland thought to hold clues, police said. Police have carried out searches of around 50 locations in London, High Wycombe and Birmingham and are continuing work at 14 sites. Though most airlines and airports were operating a full service Friday, Britain's government said there would be no return to normal airport security arrangements over the next week. The Department for Transport said it had "no intention of compromising security" by changing requirements on hand baggage in the next seven days.

Source: <http://www.cnn.com/2006/WORLD/europe/08/18/uk.terror.plot.ap/index.html>

DHS Daily Open Source Infrastructure Report Contact Information

[DHS Daily Open Source Infrastructure Reports](#) – The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open–source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website:
<http://www.dhs.gov/iaipdailyreport>

DHS Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:

Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983–3644.

Subscription and Distribution Information:

Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983–3644 for more information.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282–9201.

To report cyber infrastructure incidents or to request information, please contact US–CERT at soc@us-cert.gov or visit their Web page at www.us-cert.gov.

Department of Homeland Security Disclaimer

The DHS Daily Open Source Infrastructure Report is a non–commercial publication intended to educate and inform personnel engaged in infrastructure protection. Further reproduction or redistribution is subject to original copyright restrictions. DHS provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.